The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/16/2020

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) and Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Mozilla Thunderbird is an email client. Successful exploitation of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 84
- Mozilla Firefox ESR versions prior to 78.6
- Mozilla Thunderbird versions prior to 78.6

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) and Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A heap based buffer-overflow vulnerability. Specifically, this issue occurs due to a boundary error within WebGL component. [CVE-2020-26971]
- A security-bypass vulnerability. Specifically, this issue occurs due to insufficient validation of user-supplied input within CSS Sanitizer. [CVE-2020-26973]
- A denial-of-service vulnerability. Specifically, this issue occurs due to incorrect casting of the 'StyleGenericFlexBasis' object. [CVE-2020-26974]
- A security vulnerability. Specifically, this issue exists due to application does not properly impose security restrictions. A remote attacker can create a specially crafted webpage and send probes to hosts in internal network as well as to services on the user's local machine. [CVE-2020-26978]
- An information-disclosure vulnerability. Specifically, this issue exists due to the proxy.onRequest API does not use proxy when viewing source code of the web application. [CVE-2020-35111]
- A security vulnerability. Specifically, this issue exists due to the way Firefox processes downloaded files without extensions on Windows operating system. [CVE-2020-35112]
- A security vulnerability that occurs due to memory safety bugs. [CVE-2020-35113]

Successful exploitation of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2020-55/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-56/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-54/

CVE:
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-26971
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-26973
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-26974
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-26978

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-35111
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-35112
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-35113

Ubuntu:
https://ubuntu.com/security/notices/USN-4671-1